Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Consumer & Governmental Affairs Bureau	)	CG Docket No. 12-38
Seeks to Refresh the Record Regarding	)	
Misuse of Internet Protocol Relay Service	)	CG Docket No. 03-123
	)	
To: The Commission	)	

COMMENTS ON PUBLIC NOTICE SEEKING TO REFRESH THE RECORD REGARDING MISUSE OF INTERNET PROTOCOL RELAY SERVICE

PURPLE COMMUNICATIONS, INC.

Kelby Brick, Vice President, Regulatory
and Strategic Policy
Purple Communications, Inc.
2118 Stonewall Road
Catonsville, MD 21228

John Goodman
Chief Legal Counsel
Purple Communications, Inc.
595 Menlo Drive
Rocklin, CA 95765

March 20, 2012

REDACTED – FOR PUBLIC INSPECTION

TABLE OF CONTENTS

Purple Communications, Inc.
March 20, 2012

COMMENTS

Purple Communications, Inc. ("Purple") is pleased to provide comments related to the efforts of the Federal Communications Commission (the "Commission") to refresh the record on ways to combat misuse related to internet protocol relay service (The "2012 Notice").[1]

I. EXECUTIVE SUMMARY

Internet-based relay services ("IP Relay") are popular with deaf and hard of hearing consumers. IP Relay is a vital service for those consumers who rely exclusively on text-based forms of communication. The mobility and privacy offered by IP Relay makes it an attractive option for video relay service ("VRS") users in situations where VRS may not be available and/or may not provide the requisite degree of privacy. Unfortunately, IP Relay is susceptible to misuse.[2] Purple has worked diligently to combat illegitimate use while complying with the Commission's regulatory mandates.

Purple supports the Commission's efforts to refresh the record and address IP Relay regulation. Purple offers its experiences as a real-world "case study" of the effects of the Commission's policy decisions on the IP Relay industry and suspicious traffic in an effort to provide context for the recommendations made herein. Purple describes the tensions that providers face in endeavoring to ensure functional equivalence, satisfy the Commission's requirement to register and verify callers without unduly burdening consumers, and limit system abuses. Purple's experience shows that if the prevention of misuse is now the Commission's top priority, the Commission should (a) revisit its earlier policy decision to limit consumer burden

---

[1] *Consumer & Governmental Affairs Bureau Seeks to Refresh the Record Regarding Misuse of Internet Protocol Relay Service*, CG Docket Nos. 12-38 and 03-123, Public Notice, DA 12-208, 2012 FCC LEXIS 732 (Feb. 13, 2012) (*2012 Notice*).

[2] *FCC Fact Sheet on IP-Relay Fraud*, http://www.fcc.gov/guides/ip-relay-fraud (last visited March 18, 2012).

and (b) amend its registration and verification procedures and call handling requirements accordingly.

In these Comments, the Company explains the impact of several alternative proposals, including:

- The creation of a registration and eligibility verification system maintained by a third party;
- The establishment of more stringent regulatory registration and eligibility verification standards that offer greater protection to the industry and the TRS Fund than the Commission's current requirements; or
- The modification of mandatory call handling requirements to allow providers broader discretion to address illegitimate use.

If the Commission implements either a third-party eligibility database or increases the stringency of its regulatory registration and verification standards, it will significantly reduce illegitimate use without hindering functional equivalence.

II. CURRENT REGULATIONS CONSTRAIN THE ABILITY OF PROVIDERS TO COMBAT MISUSE.

In the 2012 Notice, the Commission requests comment regarding the measures Internet-based TRS providers currently use to verify eligibility information for registration of individuals attempting to obtain a ten-digit number and the efficacy of those methods. An understanding of the framework within which Internet-based TRS providers implement registration and verification processes is crucial to an examination of their registration and verification methods.

A. Current Regulations Have Produced a Fragmented Industry.

Providers currently face a significant tension between utilizing suitable methods for combating misuse and still complying with the Commission's requirements for call handling. Indeed, call handling requirements seriously impede providers from preventing unauthorized use because they restrict the ability of providers to monitor call content and/or terminate calls. Further, providers have received limited direction from the Commission regarding appropriate means of balancing these goals. As a result, the IP Relay industry is fragmented with different providers utilizing diverse methods (with varying degrees of stringency and success) for registration, verification and deterrence of misuse. The following provides an overview of the (1) the Commission's current mandatory call handling requirements that prioritize functional equivalence, (2) the considerations made by the Commission in restricting the current registration and verification system to not "unduly burdensome" methods only, and (3) the consequences of the patchwork of provider registration and verification practices.

1. Current Regulations Require Providers to Service Calls that May Be Illegitimate.

Based on the mandate of functional equivalency, Communications Assistants ("CAs") are prohibited from policing or refusing calls, adding to the challenges faced by providers in trying to eliminate illegitimate use of the service:

> Under the functional equivalency mandate, TRS is intended to permit persons with hearing and speech disabilities to access the telephone system to call persons without such disabilities. TRS is intended to operate so that when a TRS user wants to make a call, a CA is available to handle the call. The Commission has noted that the "ability of a TRS user *to reach a CA prepared to place his or her call* . . . is fundamental to the

> concept of 'functional equivalency.'" For this reason, the TRS regulations provide that CAs are prohibited from refusing calls.[3]

The underlying rationale for this pronouncement is that CAs should be "invisible conduits" that process calls without making independent judgments about the content of calls:

> The Commission has received complaints from vendors, consumers, and TRS providers that people are using IP Relay to make telephone purchases using stolen or fake credit cards. Although such purchases are illegal, and the Department of Justice and the FBI can investigate, *due to the transparent nature of the CA's role in a TRS call the CA may not interfere with the conversation. The TRS statutory and regulatory scheme does not contemplate that the CA should have a law enforcement role by monitoring the calls they are relaying.*[4]

Accordingly, a CA may not interfere with or disconnect from a call even when an illegal purpose of the call is apparent.

---

[3] *Telecommunications Relay Service (TRS) Providers Must Make All Outbound Calls Requested by TRS Users and May Not "Block" Calls to Certain Numbers at the Request of Consumers,* Public Notice, DA 05-2477, 20 FCC Rcd 14717, at *3 (Sept. 21, 2005) (*2005 TRS Provider Public Notice*) (citing *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CC Docket No. 98-67, Report and Order and Further Notice of Proposed Rulemaking, 15 FCC Rcd 5140, ¶ 39 (Mar. 6, 2000) (FCC 00-56) (*2000 Improved TRS Order*) (emphasis added) ("all relay services either mandated by the Commission or eligible for reimbursement from the interstate TRS Fund must comply with the mandatory minimum standards") (also citing 47 C.F.R. § 64.604(a)(3)(i) (stating that "[c]onsistent with the obligations of telecommunications carrier operators, CAs are prohibited from refusing single or sequential calls or limiting the length of calls using relay services")).

[4] *See FCC Reminds Public of Requirements Regarding Internet Relay Service and Issues Alert*, DA 04-1738, Public Notice, 19 FCC Rcd 10740, at *2-3 (Jun. 18, 2004) (*2004 Internet Relay Service Requirements Public Notice*) (emphasis added); *see also Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CG Docket No. 03-123, *Misuse of Internet Protocol (IP) Relay Service And Video Relay Service*, Further Notice of Proposed Rulemaking, FCC 06-58, 21 FCC Rcd 5478, ¶ 12 (May 8, 2006) (*IP Relay/VRS Misuse FNPRM*); *see also* 47 C.F.R. § 64.604(a)(2).

2. The Commission Balanced a Variety of Interests When Framing Current Registration and Verification Requirements.

In June 2008, when the Commission adopted a system for assigning Internet-based TRS users ten-digit telephone numbers, the Commission's primary goals included facilitating ease of routing calls, supporting the provision of 911 service, and implementing network security measures.[5] To further these goals, the Commission required providers to give consumers the capability to register with an Internet-based TRS provider as a "default provider." The Commission specifically chose not to allow users to opt out of registration because this would be inconsistent with the obligation to support E911 services.[6] The Commission also considered, but rejected, the use of a central database to store registration location information.[7] Instead, the Commission required providers to obtain location information from registered Internet-based TRS users prior to the initiation of service.[8]

The Commission considered the reduction of misuse of the system as an ancillary benefit to registration.[9] The Commission queried whether further steps could be taken to curtail such

---

[5] *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CG Docket No. 03-123; *E911 Requirements for IP-Enabled Service Providers*, WC Docket No. 05-196, Report and Order and Further Notice of Proposed Rulemaking, FCC 08-151, 23 FCC Rcd 11591, ¶ 24 (Jun. 24, 2008) (*First Internet-based TRS Order*); *see also Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CG Docket No. 03-123; *E911 Requirements for IP-Enabled Service Providers*, WC Docket No. 05-196; *Internet-Based Telecommunications Relay Service Numbering*, WC Docket No. 10-191, Notice of Proposed Rulemaking, FCC 10-161, 25 FCC Rcd 13767, ¶ 2 (Sept. 17, 2010) (*2010 TRS NPRM*).

[6] *First Internet-based TRS Order* at ¶ 44.

[7] *Id.* at ¶ 54.

[8] *Id.* at ¶ 80.

[9] *Id.* at ¶ 94.

misuse[10] and specifically sought comment on effective methods of verifying the accuracy of initial registration information to reduce the misuse of IP Relay and on further rules that might curb these problematic practices without imposing undue burdens on consumers:

> Specifically, would a closed system requiring Internet-based TRS providers to validate the registration of users before completing non-emergency calls help curb IP Relay fraud? Would such a system be possible without imposing undue burdens on legitimate Internet-based TRS users?[11]

In addition, the Commission recognized that the ability to verify the accuracy of registration information, and whether providers should be encouraged or required to block suspected illegitimate calls, were open questions. Accordingly, the Commission asked:

> And how are Internet-based TRS providers to verify that registration information itself is not fraudulent? *Absent such a mandatory system, should the Commission specifically encourage (or even require) Internet-based TRS providers to filter out requests for Internet-based TRS that come from suspected illegitimate users, such as known fraudsters or overseas users?*[12]

After evaluating comments, including those filed by consumer groups cautioning against burdensome procedures that could dissuade legitimate users from registering,[13] the Commission

---

[10] *Id.* at ¶ 95.

[11] *Id.* at ¶ 118.

[12] *Id.* (emphasis added).

[13] *See, e.g.,* Comments of Telecommunications for the Deaf and Hard of Hearing, Inc., Association of Late-Deafened Adults, Inc., National Association of the Deaf, Deaf and Hard of Hearing Consumer Advocacy Network, California Coalition of Agencies Serving the Deaf and Hard of Hearing, and Hearing Loss Association of America to *Further Notice*, Docket Nos. 03-123 and 05-196, at 18-19 (filed on Aug. 8, 2008) ("Consumer Groups") (objecting to any registration process that would be overly burdensome to relay service users, supporting instead a verification procedure that would be no more extensive than that required of voice telephone users).

addressed verification procedures associated with registration for assignment of a ten-digit telephone number.[14]

The Commission purposefully chose not to implement specific registration verification procedures. Instead, the Commission chose to "require only that Internet-based TRS providers implement a *reasonable* means of verifying registration and eligibility information *that is not unduly burdensome*."[15] Some examples, provided by commenters, that the Commission concluded were reasonable verification methods included: (1) sending a postcard to the mailing address provided by the consumer for return to the default Internet-based TRS provider;[16] (2) in-person or on camera ID checks during registration;[17] or (3) other verification processes similar to those performed by voice telephone providers and other institutions (such as banks and credit

[14] *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CG Docket No. 03-123; *E911 Requirements for IP-Enabled Service Providers*, WC Docket No. 05-196, Second Report and Order and Order on Reconsideration, FCC 08-275, 24 FCC Rcd 791, ¶ 38 (Dec. 19, 2008) (*Second Internet-based TRS Order*) (stating "To verify the accuracy of initial registration information and to help ensure that VRS and IP Relay are used only for their intended purpose, we conclude that Internet-based TRS providers must institute procedures to verify the accuracy of registration information, including the consumer's name and mailing address, before issuing the consumer a ten-digit telephone number. In addition, to ensure that registered users are aware of the eligibility limitations set forth above, the verification procedures must include a self certification component requiring consumers to verify that they have a medically recognized hearing or speech disability necessitating their use of TRS.").

[15] *Second Internet-based TRS Order* at ¶ 38 (emphasis added).

[16] *See id.* (citing TDI Coalition *Further Notice* Reply at 7) (suggesting that initial registrations could be verified "through the mail system to the registered address").

[17] *See id.* (citing CSDVRS *Further Notice* Comments at 20) (recommending that VRS applicants be required to positively identify themselves during the registration process, for example, by holding valid state or federally issued identification papers that include a photograph of the individual up to the video camera).

card companies).[18] The verification procedures and the requirement became effective on May 28, 2010.[19]

In addition to requiring that providers adopt reasonable registration verification procedures, the Commission also required that TRS providers conduct consumer education and outreach efforts to inform Internet-based TRS consumers of the importance of providing accurate registration information.[20] In taking these actions, the Commission hoped to balance the need to "reduce the misuse of Internet-based TRS by those who may take advantage of the anonymity currently afforded users, particularly IP Relay users, without unduly burdening legitimate Internet-based TRS consumers seeking to obtain ten-digit telephone numbers."[21]

3. The Restrictiveness of the Not "Unduly Burdensome" Standard and the Lack of Uniformity Among Providers Has Limited the Impact of Registration and Verification Regulations on Misuse.

Because the Commission restricted providers from obtaining registration information that may be "unduly burdensome" to consumers and chose not to mandate a specific set of verification procedures for registered users, each provider has a unique registration and verification process, with limited effectiveness. Providers have developed their processes while adhering to the Commission's mandate that processes be less than "unduly burdensome." Particularly problematic is that once any one provider registers a number and the number is registered with the iTRS database, all providers are obligated to process calls from that number.

---

[18] *See id.* (citing TDI Coalition *Further Notice* Reply at 7) (suggesting that initial registrations could be verified through the use of "processes similar to credit checks").

[19] *Telecommunications Relay Services, Speech-to-Speech Services, E911 Requirements for IP-Enabled Service Providers*, 75 Fed. Reg. 29914, 29915 (May 28, 2010).

[20] *Second Internet-based TRS Order* at ¶ 38.

[21] *Id.*

As a result, providers such as Purple with rigorous verification procedures are required to process calls from numbers registered through a potentially lax procedure.

Providers have sought rule changes that would strengthen the tools available to combat illegitimate use. For example, on October 1, 2009 one iTRS provider filed a petition with the Commission seeking to allow iTRS providers the authority to refuse to handle, disconnect or interrupt suspicious calls.[22] The Commission did not act on that petition.

In a clarification issued later in October 2009 related to ten-digit numbering, the Commission emphasized that providers must ensure that the iTRS caller is registered, or obtain registration information, before handling a call. However, once the registration information has been collected, *the provider is required to "immediately" process the call, even if the provider has not finished verifying the registration information:*

> If a caller is not registered, and is making a non-emergency call, the provider must first get the caller's necessary registration information but then must complete the call. We emphasize that the provider must handle calls to or from such callers, to the extent technically feasible, *even if the provider has not completed verifying that information*, assigning the caller a new ten-digit number, and provisioning that number to the iTRS database.[23]

The Commission further instructed providers that they must process the calls even if they have not yet assigned the ten-digit number. Specifically, "VRS and IP Relay providers must allow

---

[22] Petition for Rulemaking, *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities,* CG Docket 03-123, filed by Sorenson Communications (Oct. 1, 2009).

[23] *Consumer & Governmental Affairs Bureau Reminds Video Relay Service (VRS) and Internet Protocol (IP) Relay Service Providers of their Outreach Obligations and Clarifies their Call Handling Obligations for Unregistered Users After the November 12, 2009, Ten-Digit Numbering Registration Deadline,* CG Docket No. 03-123, WC Docket No. 05-196, Public Notice, DA 09-2261, 24 FCC Rcd 12877, at *12878-79 (Oct. 21, 2009) (emphasis added).

newly registered users to *place calls immediately after they have submitted all of the necessary registration information.*"[24]

As a result, under the Commission's current rules, providers are left with little support for preventing calls by illegitimate users. Dial-around traffic permits users to register with the least stringent provider and then use the service of any other provider. Moreover, when providers use registration and verification procedures that are not automatic and simultaneous, illegitimate users can make unlimited calls from the time they provide registration information until the time the provider detects the problem and deactivates the registration. The delay between registration and verification creates a window where unauthorized users have unfettered access to the system and they need only to fraudulently re-register once their service is deactivated to immediately place additional calls.

B. Purple Considered a Variety of Methods for Verifying a User's Registered Location, Including Those Proposed by the Commission.

The Commission seeks comment on the extent to which IP Relay providers are utilizing one or more of the methods mentioned by the Commission in the Second Internet-based TRS Order.[25] In developing its registration and verification process, Purple has considered each of the suggestions cited by the Commission. The following summarizes Purple's analysis with respect to each proposal.

[24] *Id.* at n.14 (emphasis added).

[25] *2012 Notice* at *14.

1. The Company Considered Postcards but Determined That Verification By Postcard Created An Unacceptable Window For Illegitimate Use and Potential for Error.

Purple considered sending a postcard to the mailing address provided by a registered customer for return to Purple. However, such a process involves delays of days or weeks and creates an unacceptable window of time during which an illegitimate user may have access to the service. Further, once Purple blocked a user that failed a postcard verification procedure, the user need only re-register with a new stolen identity to begin placing calls again for the duration of a subsequent verification window. This cycle could continue indefinitely. Requiring customers to provide a copy of a utility bill would create the same window of opportunity for misuse.

Postcards have additional drawbacks and potential for error. First, if an illegitimate user provides a name and address from a phone book or other publicly-available source, the Post Office will deliver the postcard and not return it to the provider. Accordingly, providers cannot rely on a "return to sender" bounce-back from the Post Office for purposes of verification. Second, a system that requires the return of a postcard by a customer may risk frequent deactivation of legitimate accounts. For example, customers may simply fail to recognize a postcard among large quantities of mail or may not distinguish the postcard from other advertisements. Some sources report that an average of 41 pounds of junk mail is sent to every adult citizen each year, and approximately 44% of this mail goes into a landfill unopened.[26] Postcards are unlikely to be signed and returned by consumers with any regularity. Further, without the privacy of an envelope, the content of postcards is within the public view and

[26] *Junk Mail Impact,* http://www.41pounds.org/impact/ (last visited Feb. 23, 2012).

exposes customers to privacy concerns and increased risk of identity theft. Given the limited likelihood of success and other concerns listed, Purple determined that postcards are not an optimal method of reliably confirming customer name and address information.

2. In-Person or On-Camera ID Checks Are Not Always Feasible.

Verifying a user's identity through on-camera ID checks, while useful for verifying VRS users, is impractical for verifying many IP Relay users. VRS users can easily show their ID on-camera because they are signing up for a service that requires the use of video phones or other video chat enabled technology. Many IP relay users will not have easy access to such technology. IP Relay users are very often persons who are not ASL proficient. Such persons may have become deaf or hard-of-hearing later in life or may never have learned ASL.[27] Such customers cannot use VRS and are thus less likely to have or be able to use video phones or other video-enabled technology.

Verifying a user's name and address information through in-person ID checks may not be feasible for many remote and immobile users. Customers would have the burden of traveling to register or providers would have to invest significant manpower to reach rural and limited-mobility users. Therefore, such a requirement would likely dissuade many legitimate users from registering and/or be cost prohibitive to providers and to the TRS Fund.

3. Verification Processes in Other Industries are Unsuitable for IP Relay Because They Serve a Different Purpose.

The Commission's other proffered example of "verification processes similar to those performed by voice telephone providers and other institutions (such as banks and credit card

[27] *See* Steve Barber, *Deaf and Hard of Hearing*, Hearing Loss Association of North Carolina, http://www.nchearingloss.org/article_demographics.htm (last visited Feb. 23, 2012).

companies)" also fails to result in a reasonable or appropriate verification procedure for IP Relay customers. While Purple acknowledges that some of the data gathered by these entities could pertain to user identity, the ultimate purpose of verification measures of voice telephone providers, banks and credit card companies differs from simple name and address verification. For example, telephone providers, banks and credit card companies make use of their procedures to assess the creditworthiness of account applicants. By contrast, the creditworthiness of IP Relay users, a significant number of whom are under-educated, elderly, and disproportionately poor, is not relevant to name and address verification. Accordingly, the use of databases designed to determine creditworthiness could be overreaching, imposing and burdensome to the typical IP Relay consumer and unreasonable in the context of the population being served. Many legitimate users simply may be unwilling to provide this type of information.

C. No Established Process Exists to Obtain an Alternative Means of Verification Approved in Advance by the Commission.

The Commission also seeks comments on alternative means of verification approved in advance by the Commission. Unfortunately, Purple is not aware of any process by which a provider could seek such pre-approval from the Commission. In fact, Commission employees repeatedly have informed Purple that they are not allowed to speak to providers on behalf of the Commission regarding verification procedures. Purple believes that while such a process would have been commendable, it was not available. In any event, as discussed above, if one provider were to use a more restrictive method than the methods implemented by other providers, users (including legitimate customers) may choose a provider with a less intrusive and burdensome process. This would significantly impair the value of *ad hoc* approval of provider-specific registration and verification processes.

D. Purple has Developed a Simultaneous Registration and Verification Procedure That Works in Conjunction with an Effective Process for Identification and De-Registration of Illegitimate Users.

The Commission seeks comment regarding the effectiveness of the registration and verification measures actually implemented by providers to screen out illegitimate IP Relay users. While not initially acknowledged by the Commission, the requirement that providers process non-emergency calls following registration *even if* verification is pending constructively requires that providers develop simultaneous registration and verification procedures. The limitations of the proposals outlined above left reasonable providers with little choice but to develop their own effective measures to combat misuse while still adhering to the applicable regulations and the requirement that processes not rise to the level of "unduly burdensome". Purple has and continues to invest substantial efforts in developing an industry-leading instant registration and verification solution.

1. Purple Uses Instantaneous Registration and Verification to Combat Illegitimate Calls.

When registering with Purple, a caller is required to provide certain information. For example, when registering [redacted]

[redacted]

[28] [redacted].

[redacted]

After a customer is registered, Purple sends the user an e-mail requesting that s/he click on a link to certify that the identity information s/he has provided during registration is true and correct. If the user does not certify accuracy of the identity information provided at registration by clicking the emailed link within 30 minutes, Purple deactivates the user's ten-digit number. While this process requires a 30-minute delay between the registration and the email verification, it provides an additional level of assurance to Purple's customer identity verification process.

[redacted]. These instantaneous checkpoints must each be satisfied before a caller can reach a CA. Simultaneous registration and verification offers efficiency, effectiveness and a first line of defense against misuse because it takes place before any calls are placed.

[29] [redacted]

2. Purple Also Uses State-of-the-Art Post-Registration Methods to Promptly Identify and Eradicate Illegitimate Users of the Service – Including Dial-Around Customers.

[redacted][30]

Purple also has developed a system for manually scrutinizing registration information to make an immediate and personalized assessment about whether registered users are legitimate. Investing in a team of seasoned professionals highly familiar with the practices of illegitimate users, Purple analyzes registrations and both deregisters and blacklists users who have registered with what appear to be suspicious or illegitimate information.

E. Current IP Relay Regulations Limit Purple's Options for Combating Misuse.

The Commission asks whether individuals outside of the U.S. have been obtaining IP Relay access numbers or otherwise using the service unlawfully, as well as to what extent current provider practices enable or contribute to the registration of ineligible IP Relay users. While Purple has developed the above-described verification process, including use of an instantaneous

30 [redacted]

verification database, illegitimate users may still evade registration and verification requirements because the Commission chose to limit registration requirements to only those that are not "unduly burdensome" to consumers. As a result, Purple's post-registration measures are an essential part of Purple's overall verification system for preventing misuse of the service. Indeed, the post-registration measures of Purple's verification process are so effective that in 2011, Purple deactivated over 80% of its newly-registered IP Relay users.

1. Identity Theft Poses Problems for Registered Location Verification.

Even an instantaneous registration and verification procedure such as Purple's system has limitations. Although "Registered Location" verification procedures are required by current registrations, such procedures can be overcome by illegitimate users willing to commit identity theft. Purple's experience shows that even the addition of name, address, and e-mail address verification is insufficient to prevent illegitimate users from accessing the service entirely. Illegitimate users need only to enter an accurate, albeit stolen, name and address from a telephone book and set up a web-based e-mail account to register. For this reason, and of its own volition, Purple has added a birth date matching requirement to all registrations via AIM.

2. Dial-Around Traffic Undermines Registration and Verification Efforts.

Purple understands the value of dial-around capability to consumers. However, even if Purple's registration and verification regulations permitted only legitimate users to register, the Commission's rules still require Purple to process calls from illegitimate users registered with other providers. Purple has no control over the sufficiency and effectiveness of the registration and verification processes of other providers. Therefore, unless all providers use uniform

verification processes, individual providers will remain exposed to illegitimate calls. For these reasons, Purple suggests the Commission adopt universal guidelines for IP Relay registration.

3. Proxy-Encryption Services Present a Challenge to Blocking International Callers.

The Commission seeks comment on whether advanced call-tracking mechanisms – e.g., geolocation systems – are available for the purpose of accurately determining whether a particular IP Relay call is originating from or terminating to an international location. Geolocation systems are a minimal requirement for all providers. However, many legitimate consumers access IP Relay through the popular AIM platform. Unfortunately, AIM can function as a proxy-masking service, and rendering geolocation systems ineffective.

Purple contacted AOL, Inc. in an effort to broker a more transparent system that reveals the true location of the IP addresses of AIM users. AOL cited technical and financial reasons for declining Purple's request. Without AOL's cooperation, the industry should explore means of combating the potential for misuse conducted over AIM, such as stronger registration and verification procedures and a rule restricting an AIM caller's ability to place more than one IP Relay call at a time.

III. PURPLE'S EXPERIENCE SUPPORTS NEW RULEMAKING.

The Commission seeks input on what additional steps should be taken to prevent the registration and use of IP Relay by ineligible callers. First and foremost, if it is the Commission's policy to re-prioritize combating misuse of the system, it cannot continue to constrain the burden of registration and verification on consumers in the same manner. The Commission needs to require consumers to provide more than just E911 address information

when registering for Internet-based TRS. With that in mind, Purple proposes three regulatory options that will substantially reduce misuse of the service by illegitimate users.

A. Best Practices Require IP Relay Users to Register Through a Third Party.

A more rigorous centralized registration and verification process will offer the most effective system to combat illegitimate use while serving consumers and providers. Similar to its proposal in the Commission's VRS reform proceeding[31], Purple recommends that the Commission assign the task of registering and verifying eligible IP Relay users to a third party, rather than delegate this responsibility to the providers. The third party will register and verify IP Relay caller eligibility using standardized and uniform procedures and assign each verified user his/her ten-digit number. User information, including ten-digit numbers and E911 registered locations, should then be stored in a universal database maintained by the third party. IP Relay providers should be able to access callers' ten-digit numbers and E911 Registered Locations only from the universal database. Use of a third party for registration and verification purposes, as well as ten-digit number issuance and maintenance, will homogenize the industry's approach to misuse and ensure that confidential user eligibility information is protected.

1. Establishing a Third-Party Uniform Verification Process Will Allow Consumers the Benefits of Choice and Will Eliminate Conflicting Incentives Among Providers.

High-quality service and technological advances are closely tied to competition and consumer choice. The presence of a uniform registration and verification protocol eliminates any questionable incentives that may exist related to the registration and handling of suspicious

[31] Purple's Comments to FNPRM on Structure and Practices of the Video Relay Services Program, CG Docket No. 10-51, CG Docket No. 03-123, at p. 11 (filed March 8, 2012) (proposing a centralized and independently managed registration and database approach).

callers. By unifying the registration and verification process and placing it under the control of a third-party manager, the Commission maintains consumer choice while ensuring that providers are only focused on serving customers who have passed effective verification. Centralizing registration also simplifies user experience as consumers will only need to enter information into a single system.

2. Requiring a Single Third Party to Register and Verify Users Will Ensure Effective and Consistent Implementation of Registration Procedures and is Attractive to Users and Providers Alike.

Even if the Commission establishes uniform registration and verification requirements that apply to each provider, there is no guarantee that each provider would implement the requirements the same way. Accordingly, assigning the task of registering users to a disinterested third party creates the only guarantee of a truly uniform solution.

IP Relay providers should support third-party eligibility determination because it will reduce the costs associated with providing IP Relay services. The process will also restrict access by illegitimate callers, decreasing the need for providers to deploy extensive post-registration efforts to identify illegitimate users. Finally, having eligibility status determined by a third party could preserve for consumers the ability to utilize dial-around services because the entire industry will use one universal source of reliable eligibility information.

Consumers would further benefit from a third-party assessment. First, confidential eligibility information will not be held by IP Relay providers. With a third-party database solution, providers will need access only to a user's ten-digit number and his/her E911 address. Such a process will afford users greater anonymity and protect their privacy rights. Customers will also be able to change default providers with greater ease, as they will not have to port their

ten-digit numbers when they move between providers. Finally, as discussed in detail below, a third-party universal database will obviate the need for call-monitoring and/or modification of the Commission's call handling requirements thereby ensuring even greater functional equivalence for consumers.

3. A Centralized System will Prevent Most Illegitimate Use and Obviate the Need for Post-Registration Procedures.

The Commission seeks comments on whether CAs should be given the discretion to determine, on a case-by-case basis, that a call is not a legitimate TRS call, and to block, terminate, or refuse to handle a call. Purple believes that such measures are unnecessary if the Commission requires IP Relay users to register with and have their eligibility confirmed by a third party. If illegitimate users are prevented from accessing the system because of clear registration and verification requirements implemented by a neutral third party, there may be no need to compromise call confidentiality or monitor call content.

B. Alternatively, the Commission Should Mandate that All Providers Use a Proscribed Registration and Verification Method.

For the reasons set forth above, a registration and verification method uniformly applied to all IP Relay providers and consumers is the best means to prevent illegitimate users from registering for and using IP Relay and the referred option for consumers, providers, and the Commission. However, if the Commission does not assign registration and verification to a third party, the Commission should establish clear and specific mandates that providers must follow when registering users. A system that relies on IP Relay providers is not as secure as a system that relies on a third party to register users. Further, in this framework, users are still required to

submit sensitive registration information to providers, which removes a level of privacy and anonymity offered by a third-party maintained database.

C. Purple Recommends the Following Registration and Verification Requirements Whether Conducted by a Third Party or by Providers.

For the reasons discussed herein, a universal registration and verification process—whether it is a centralized third-party system or a uniform program implemented at the provider level—is critical for preventing illegitimate use of Internet-based TRS. Purple outlines below its recommendations for the types of information that the Commission should require consumers to provide as evidence of their eligibility for enrollment.

1. Together with Consumer Groups, the Commission Should Consider Requiring Users to Prove Their Eligibility to Use IP Relay.

The Commission should revisit with consumer groups the additional steps that should be taken to ensure customer eligibility for IP Relay. If preventing misuse is the Commission's priority, the Commission should require users to prove that they have a disability in order to register for IP Relay. Proof of eligibility will further the ability of providers to help ensure only legitimate users place IP Relay calls and strengthen the security of the TRS Fund. Requiring a doctor's note or similar evidence (e.g. confirmed enrollment in another program for which disability is an eligibility criterion) will reduce the capability of illegitimate users, especially illegitimate users located outside of the United States, to register for IP Relay. Consumers also will benefit from fewer illegitimate users because hearing individuals receiving IP relay calls will be more willing to accept calls when suspicious calls are less prevalent.

Purple cautions, however, that some consumers may find such a requirement invasive. Nonetheless, Purple recognizes that it is up to the Commission to work with consumer groups to

address privacy concerns in light of the value of such a requirement to protecting the integrity of the TRS Fund.

2. The Commission Should Establish More Rigorous Identification Requirements.

Verifying a user's registered location, while not "unduly burdensome" to consumers, is insufficient to prevent illegitimate users from registering. Because name and address information is readily available to individuals willing to commit identity fraud, Purple recommends that the Commission require more stringent identity verification requirements irrespective of whether the Commission requires users to provide evidence of their qualifying disability. Specifically, the Commission should consider requiring a consumer to provide his/her name, address, full or partial social security number and date of birth at the time of registration. Such information should be instantly confirmed through an appropriate database prior to the placement of any non-emergency calls.

The Commission should consider allowing users to choose the method of identity and/or address verification. Those users willing and able to provide social security numbers could gain immediate access to IP Relay. Those users uncomfortable providing social security numbers could instead gain immediate access to IP Relay by charging a nominal fee to a credit card thereby verifying their addresses. Those users unconcerned with immediate registration, or who wish to provide neither a social security number nor a credit card number, could mail, fax or e-mail a copy of their identification information. Under any scenario, Purple recognizes the value of including consumer groups in establishing a framework that is effective and not unduly burdensome.

D. Permitting a Patchwork of Registration and Verification Procedures Will Require Changes to Call Handling Rules and Significant Post-Registration Interventions by Providers.

If the registration process is not centralized and/or made uniform, the rules should be changed to allow CAs to monitor call content and terminate suspicious calls. However, Purple emphasizes that such changes to call handling requirements offer neither a workable solution, nor a significant improvement over the current framework. Given current regulations, Purple's sole option has been to devote substantial resources to post-registration procedures. Nonetheless, such post-registration procedures will never be as effective as preventing illegitimate callers from registering at the outset. Should the Commission decide not to establish a centralized database and/or uniform registration and verification procedures, it should require that providers review [redacted]. The Commission should also adopt rules that expressly allow CAs and/or their supervisors to terminate suspicious calls. Providers should also be required to maintain blacklists of illegitimate users and report suspicious call content regularly so that the Commission can create a database of illegitimate user information and dictate a uniform set of illegitimate call indicia upon which all providers can rely. Given the constant evolution of the tactics of questionable callers, Purple suggests frequent information sharing among providers and the Commission so that abusive call indicia are consistently tracked and updated.

IV. A UNIFORM REGISTRATION SYSTEM WILL REQUIRE FEW ADDITIONAL MEASURES TO COMBAT ILLEGITIMATE USE.

In light of the apparent misuses of IP Relay, the Commission inquires whether it should continue to permit temporary authorization for a user to place IP Relay calls while verification of the caller is taking place. For the reasons set forth earlier in these Comments, the Commission should not allow users to make non-emergency calls until their registration information has been verified. Regardless of the registration and verification system that is in place, any temporary authorization is a means by which illegitimate users can access the system. Given the limitations of the current framework, Purple also encourages the Commission to require that all users be re-verified in a manner consistent with any revised registration and verification regulations.

The Commission seeks comment concerning whether providers should be required to maintain and submit documentation regarding illegitimate calls to better facilitate program oversight. So long as the Commission adopts a more effective means of restricting the accessibility of the system to illegitimate users, such recordkeeping is unnecessary. However, Purple supports the inclusion of merchant complaints regarding illegitimate calls on provider's annual complaint logs, in part because such reporting will provide a good metric of the success of any new registration and verification system in effect.

The Commission also seeks comment regarding whether more rigorous user authentication on a per-call basis should be employed to combat misuse of IP Relay. Per call authentication process is not necessary if the FCC implements a centralized and/or uniform registration process. It likely would interfere with expeditious call handling and negatively impact provider service standards. Furthermore, per call verification results in inefficiencies and

unnecessary expense because it essentially requires re-registration before every call. Such a practice would also do little to limit the accessibility of the system to illegitimate callers without substantial amendment to current registration and verification criteria.

Finally, if registration is made uniform and providers are not required to allow users to make calls before they verify the user's information, no additional auditing practices will be necessary to improve the industry.

V. IP RELAY REMAINS A CRITICAL SERVICE FOR THE DEAF AND HARD-OF-HEARING.

IP Relay service is vital to deaf and hard-of-hearing individuals who are not ASL proficient. Indeed, the majority of the deaf population is not ASL proficient, including: individuals who became deaf later in life as well as individuals who never learned to sign. IP Relay is quite similar to two-way messaging (a preferred form of communication among the deaf) and is simple to use.

ASL-proficient VRS users also make regular use of IP Relay under certain circumstances. For instance, should an ASL-proficient user require privacy during a call to a hearing user (e.g. a doctor) that s/he is making in a public place, s/he may wish to use IP Relay instead of VRS. This will ensure that no one will observe the caller signing a message to his/her mobile device.

Finally, Purple notes that the industry has experienced a migration of TTY users to IP-services as broadband has become more affordable. Purple expects this trend to continue in the future.

VI. SUMMARY

Given both the regulatory landscape and Purple's experience as a leading IP Relay provider, it is clear that the ADA, the TRS Fund, the industry and consumers would all be better served by strengthening the process of registering and verifying users who wish to access IP Relay. Purple commends the Commission for the thoughtful proposals in the 2012 Notice. Purple believes that the Company's proposals, if adopted, can meaningfully improve the current model. Purple welcomes the opportunity to work with the Commission and other stakeholders to address the challenge of combating illegitimate use of the system, while maintaining the highest quality service at the lowest possible cost, preserving consumer choice, and serving the mission of functional equivalence.